NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ROBUST DEFENSE AGAINST SMALL BOAT ATTACKS

by

Ka-Yoon Wong

December 2010

Thesis Advisor: Thomas W. Lucas
Second Reader: Jeffrey E. Kline

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2010	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE Robust Defense Against Small Boat Attacks		**5. FUNDING NUMBERS**	
6. AUTHOR Ka-Yoon Wong			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number N/A.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE: A

13. ABSTRACT (maximum 200 words)

Nearly a decade after the small boat attacks against the USS Cole (in 2000) and M/V Limburg (in 2002) in Yemen, small vessels continue to pose a security threat. In part, this is due to the ease of camouflage and the high frequency of small vessels operating in proximity to important maritime infrastructure, such as bridges and petrochemical plants, and to passenger and military ships. In this study, small boat effectiveness in the interception of attacking speedboats is analyzed using the stochastic, time-stepped, agent-based simulation tool MANA. Three alternative defender tactics of scramble from base, barrier patrol, and random patrol are explored against two possible attacker modus operandi of saturation attack and diversionary attack. The probability of at least one attacker reaching the defended asset is the primary measure of effectiveness. A full factorial experiment was designed and executed for defenders tasked to protect the Port of Los Angeles and the Port of Hong Kong. The findings indicate that the defenders are highly susceptible to diversionary attacks regardless of tactics employed, but their effectiveness can be improved by retaining sufficient defensive assets in preparation for a potential follow on attack. The study highlights the limits on patrol boat effectiveness to intercept small high speed vessels which lead to the nullification of any numerical advantage the defender may have when faced with a saturation attack. Anticipating the heading of the attacker is a critical factor for a successful engagement.

14. SUBJECT TERMS Maritime Security, Critical Infrastructure Protection, Small Boat Attacks, Simulation, Optimization	15. NUMBER OF PAGES 65
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

i

THIS PAGE INTENTIONALLY LEFT BLANK

ROBUST DEFENSE AGAINST SMALL BOAT ATTACKS

Ka-Yoon Wong
Defence Science and Technology Agency, Singapore
B.Eng (Hons), Nanyang Technological University, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN OPERATIONS RESEARCH

from the

NAVAL POSTGRADUATE SCHOOL
December 2010

Author: Ka-Yoon Wong

Approved by: Thomas W. Lucas
                   Thesis Advisor

                   Jeffrey E. Kline
                   Second Reader

                   Robert F. Dell
                   Chairman, Department of Operations Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Nearly a decade after the small boat attacks against the USS Cole (in 2000) and M/V Limburg (in 2002) in Yemen, small vessels continue to pose a security threat. In part, this is due to the ease of camouflage and the high frequency of small vessels operating in proximity to important maritime infrastructure, such as bridges and petrochemical plants, and to passenger and military ships. In this study, small boat effectiveness in the interception of attacking speedboats is analyzed using the stochastic, time-stepped, agent-based simulation tool MANA. Three alternative defender tactics of scramble from base, barrier patrol, and random patrol are explored against two possible attacker modus operandi of saturation attack and diversionary attack. The probability of at least one attacker reaching the defended asset is the primary measure of effectiveness. A full factorial experiment was designed and executed for defenders tasked to protect the Port of Los Angeles and the Port of Hong Kong. The findings indicate that the defenders are highly susceptible to diversionary attacks regardless of tactics employed, but their effectiveness can be improved by retaining sufficient defensive assets in preparation for a potential follow on attack. The study highlights the limits on patrol boat effectiveness to intercept small high-speed vessels which lead to the nullification of any numerical advantage the defender may have when faced with a saturation attack. Anticipating the heading of the attacker is a critical factor for a successful engagement.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Nearly a decade after the small boat attacks against the USS Cole (in 2000) and M/V Limburg (in 2002) in Yemen, small vessels continue to pose a security threat. In part, this is due to the ease of camouflage and the high frequency of small vessels operating in proximity to important maritime infrastructure, such as bridges and petrochemical plants, and to passenger and military ships.

According to an analysis spanning four ports (Abdul-Ghaffar, 2008), an intelligent enemy executing an attack using explosives-laden speed-boats, who is able to observe the defense and choose an attack route to maximize the probability of evasion, can be detected with near certainty. Through the application of an attacker-defender bi-level optimization mixed integer program, the author recommended the pre-positioning of patrol boats to achieve a near 100% probability of detecting an approaching small vessel, but noted that the interception of the attackers may not have been possible with the proposed positions as interception was not an objective of his model. In addition, since Abdul-Ghaffar was essentially stationing picket boats to provide best sensor coverage, he suggests his solutions need augmentation through future research on the solution for best intercept tactics. Operationally, these tactics imply mobile patrol sectors located near expected threat axes or choke points vice stationary picket locations.

This thesis expands on Abdul-Ghaffar's prior research, illustrating the use of modeling and simulation to analyze the robustness of the recommended deployment profile in interdicting the threat. The effectiveness of three alternative defender tactics (scramble from base, barrier patrol, and random patrol) are explored against two possible attacker modus operandi of saturation attack and diversionary attack using the stochastic, time-stepped, agent-based simulation tool MANA. The primary measure of effectiveness is the probability of at least one attacker reaching the defended asset. A full factorial experimental design was conducted for defenders tasked to protect the Port of Los Angeles and the Port of Hong Kong.

The analysis raised several key issues concerning the interception operation:

- **Defenders are highly susceptible to diversionary attacks:** Regardless of defenders' tactics, if a decoy boat manages to divert the attention of the defenders, the real attacker would be able to slip through and deliver a nasty blow to the defended asset. The defender must be prepared for the likelihood that the attacker will employ a diversionary tactic by retaining sufficient defensive assets for a potential follow on attack.

- **Patrol boat effectiveness is limited:** Weapons fired from a moving platform may not hit their mark due to the instability of the moving platform, coupled with the fact that both the patrol boat and attacker are maneuvering, limiting the effectiveness of the patrol boat in stopping an attacking small vessel. In addition, the cloud of confusion that can arise in the melee when defenders give chase to multiple attackers could lead to one or more attackers getting through to the defended asset.

- **Saturation attack nullifies defenders' numerical advantage:** Due to the limited effectiveness of the patrol boats described above, the defenders' numerical advantage may not be realized when facing multiple attackers, particularly if the attack is concentrated along a single axis.

- **Anticipating the attacker's heading is a critical to successful engagement**: In this study, the defenders are able to anticipate where the attackers will head toward since the defended assets are confined to a small geographical location. The defenders will be disadvantaged if the defended assets stretch over a long coastline.

This research demonstrates the use of modeling and simulation to facilitate understanding the interception of small boat attacks using several possible defensive tactics, and has spotlighted key limitations in the defense. The complexity of the problem calls for further research on aspects of interception operations not studied in this thesis, such as to understand the factors pertinent to the defense of assets spread over a longer coastline, or to assess alternative platforms and weapons for more effective mitigation of the small boat attack threat.

ACKNOWLEDGEMENTS

Professor Lucas, thank you for the guidance and sharpening of my focus on the core issues. It has been a great honor to work with someone whose work I only used to read about from afar.

Meredith Thompson and Mary McDonald of the SEED Center, deepest appreciation for your responsive technical support in my simulation runs, you've eased my stress by orders of magnitude. Heartfelt thanks to Ben Anderson, Jon Macaskill, Jesse Lorenzen for being there to sharpen ideas and giving the operator's perspective on many issues.

Siow Hiang, Yang How and Yeaw Lip, it is only by your support that I've been able to pursue my Master's degree here at NPS. Thank you for your confidence and faith in me.

To my excellent wife Ruth, thank you for the joy of going on life's adventure together, wherever, and for the immeasurable love and support as I completed this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. CLEAR AND PRESENT DANGER

The Department of Homeland Security (DHS) defines small vessels as:

Any watercraft, regardless of method of propulsion, less than 300 gross tons (GT). Small vessels can include commercial fishing vessels, or any other commercial vessels involved in foreign or U.S. voyage…. Although there is no exact correlation between a vessel's length and its gross tonnage, a vessel of 300 GT is approximately 100 feet in length. (DHS Small Vessel Security Strategy (SVSS), 2008, p. i)

Nearly a decade after the attacks against the USS Cole (in 2000) and the M/V Limburg (in 2002) in Yemen, attacks involving small vessels remain an extant maritime threat, especially when small vessels are "readily vulnerable to potential exploitation by terrorists, smugglers of weapons of mass destruction, narcotics, aliens, and other contraband, and other criminals" (DHS SVSS, 2008, p. i).

The same report quoted that there are "nearly 13 million registered U.S. recreational vessels, 82,000 fishing vessels, and 100,000 other commercial small vessels" (p. 9) operating in U.S. waters, and "perhaps another 4 million unregistered recreational boats" (p. 9). The ease of a threat camouflaged in the midst of numerous small vessels, compounded by the high frequency of small vessels operating in proximity to important maritime infrastructure, such as bridges and petrochemical plants, and to passenger and military ships, make small vessels a continuing security concern.

According to an analysis spanning four ports (Abdul-Ghaffar, 2008), an intelligent enemy executing an attack using explosives-laden speed-boats, who is able to observe the defense and adjust accordingly, can be detected with near certainty, but the author noted that the interception of the attackers may not have been possible. Of course, if an attack has been detected, it is imperative to intercept and stop the attack.

B.   RESEARCH DIRECTION

With the interest from DHS in addressing the threat from small vessels and a gap of understanding concerning interception, this research is guided by the following goals:

1.   Analyze the effectiveness of previously recommended patrol boat locations (by Abdul-Ghaffar, previously optimized for surveillance) in an interception operation.

2.   Exploratory analysis of alternative defender tactics against a variety of attacker tactics to obtain insights into the interception operation, with regards to:

   a.   Optimal strategies to employ defender assets, and

   b.   Possible weaknesses the attacker can exploit.

C.   THESIS FLOW

The thesis is organized as follows: Chapter II paints a backdrop by detailing the prior analysis that was performed by Abdul-Ghaffar. An in-depth discussion is made on the operational implications of the findings and the link to the motivation of this study. Chapter III surveys the expected operational environment, relates current security strategies and a precise threat definition, and translates attackers' and defenders' concept of operations (CONOPS) into the simulation model. Chapter IV presents a detailed discussion of the results and relates the simulation results back to the real world. Chapter V concludes the analysis with operational insights and compares the simulation methodology used to Abdul-Ghaffar's attacker-defender model, with a proposal of topics for further research.

II. BACKGROUND AND MOTIVATION

A. PRIOR ANALYSIS

Abdul-Ghaffar (2008) developed a planning tool that recommends the positions of SAFE Defender-class patrol boats as surveillance picket ships to detect determined adversaries attacking known high-value assets in ports with small boats. Due to the accessibility of the ports to the public, the attackers were deemed to have the capability to obtain "prior knowledge of the defensive disposition" (Abdul-Ghaffar, 2008, p. xvii). His objective was to achieve an "optimal pre-positioning of defender surveillance pickets to protect high-value assets to minimize the maximum probability that intelligent attackers, observing our surveillance positions, can evade us" (p. 57). He successfully showed that "in every instance… alert defenders with existing radar can detect attacker raids with near 100% probability via their optimal pre-positioning. This is due to the restricted navigational access channels to ports" (p. 57). However, he conceded that the interception of a detected attack may not be possible "due to the relative speeds of the defending pickets and the attacker craft" (p. xviii). In addition, the intercept geometry between the attacking boats and the defender platforms, whose positions were optimized for detection, may not have been optimal for interception.

B. MODEL OVERVIEW

Using the probability that an attack will be detected as a Measure of Effectiveness, Abdul-Ghaffar modeled the terrain of a port as a mesh network (see Figure 1), where nodes represent square cells of 0.15 nautical miles (NM) by 0.15NM, and edges represent the accessible neighboring cells.
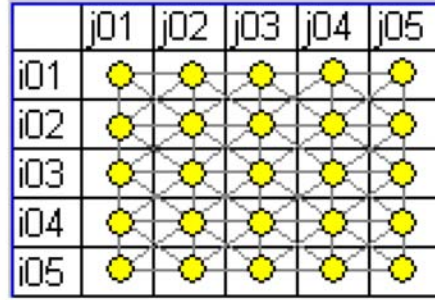
Sample network representation with square cells of constant width, each identified by a row and a column index. An attacker can traverse from any cell via an arc to any adjacent cell.

Figure 1.   Network Representation of Port Terrain (Abdul-Ghaffar, 2008)

The attacker's goal was to choose an attack route to minimize the probability of being detected, being able to exploit weaknesses in the defense through the prior observation of defensive preparations. The defender's task was to position defender patrol boats, which function as surveillance platforms, so as to collectively "minimize the maximum probability of evasion by the attackers" (Abdul-Ghaffar, 2008, p. 17).

The probability of detection was modeled using the radar range equation (Skolnik, 2002), taking into consideration obstacles that may obstruct the line of sight between the patrol boats and the attackers. The problem was then formulated as an attacker-defender bi-level optimization mixed integer program, and subsequently decomposed and solved as a capacitated network flow linear program using the General Algebraic Modeling System (GAMS, 2008).

C. VARIABLES AND TECHNICAL SPECIFICATIONS

The defender platform considered was SAFE Boats International's Defender class patrol boat, a standard boat in the United States Coast Guard (USCG, 2010), while the attacker was assumed to use a Baja 20' Outlaw class speedboat (see Figure 2).

Baja 20' Outlaw Class	
Length	20'4" - 6.2 m
Beam	7'10" - 2.39 m
Weight	2,900 lb - 1,315 kg
Weight w/ explosives	3,900 lb
Draft	34" - 86.36 cm
Fuel Capacity	50 gal - 170.3 L
Passenger Capacity	6
Max speed	54.2 knots
Attack Range w/RPG	200m

SAFE Defender Class	
Length	25' - 7.62 m
Beam	8'6" - 2.59 m
Draft	3' – 0.91 m
Fuel Capacity	50 gal - 170.3 L
Crew	4
Max Capacity	10
Max speed	46 knots
Radar	Furuno 4 kW radar Range (36 NM)
Armament	Effective Range
One 12.7 mm machine gun	1500 m
Capabilities	Detect & Intercept

20' Baja Class Specifications (From: Baja Marine, 2008). SAFE Defender Class Patrol Boats (From: SAFE, 2003).

Figure 2.   Technical Specifications of Baja Outlaw and SAFE Defender (Abdul-Ghaffar)

D. RESULTS OF THE PRIOR ANALYSIS

Abdul-Ghaffar analyzed four ports, namely the Port of Los Angeles (LA), the Port of Hong Kong (HK), Al-Basra oil terminal in Iraq, and the US 5th Fleet Headquarters in Bahrain. The number of attackers ranged between one and four, with the ports defended by either two or four defenders. Figures 3 through 6 show some of Abdul-Ghaffar's recommended deployments of the patrol boats, all of which achieved a 100% rate of detecting the intruder. The patrol boats in some scenarios appear co-located, while in

other scenarios, the attackers are observed to choose similar attack routes. The implications arising from these two observations will be discussed in greater detail in the following section.
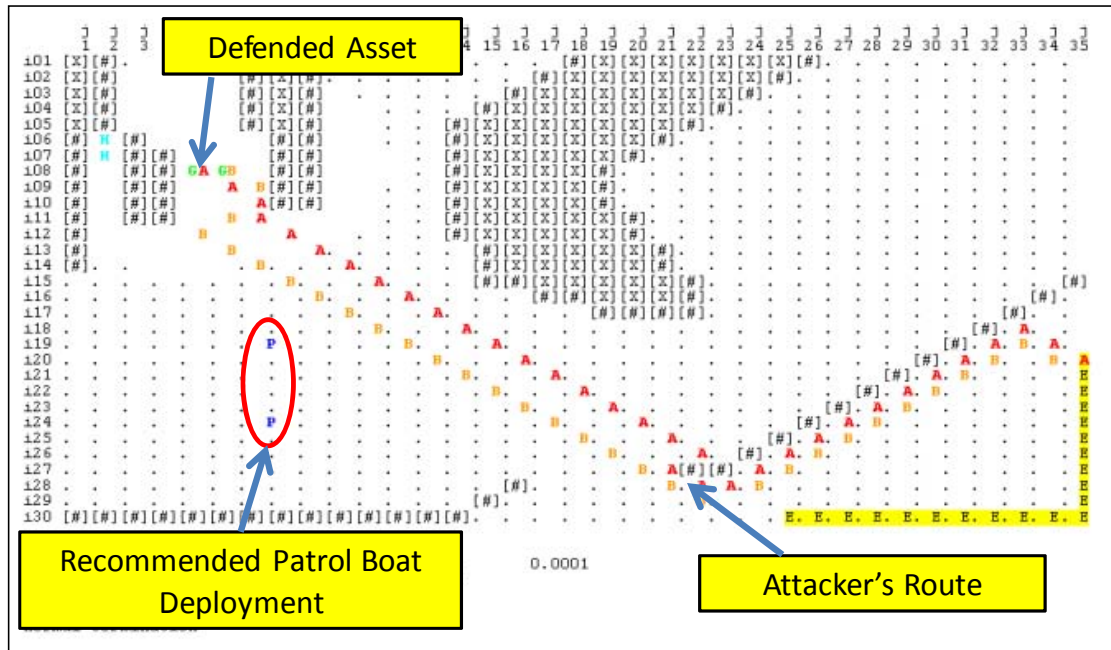

Figure 3.   2 Defenders Against 2 Attackers in LA (After Abdul-Ghaffar, 2008)
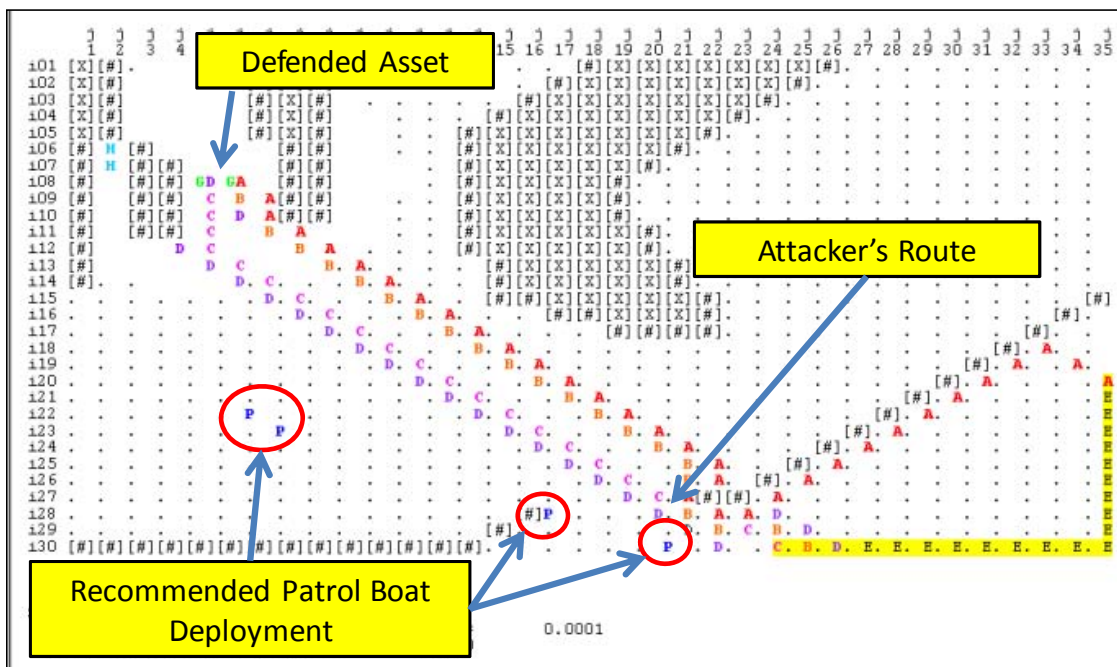

Figure 4.   4 Defenders Against 4 Attackers in LA (After Abdul-Ghaffar, 2008)
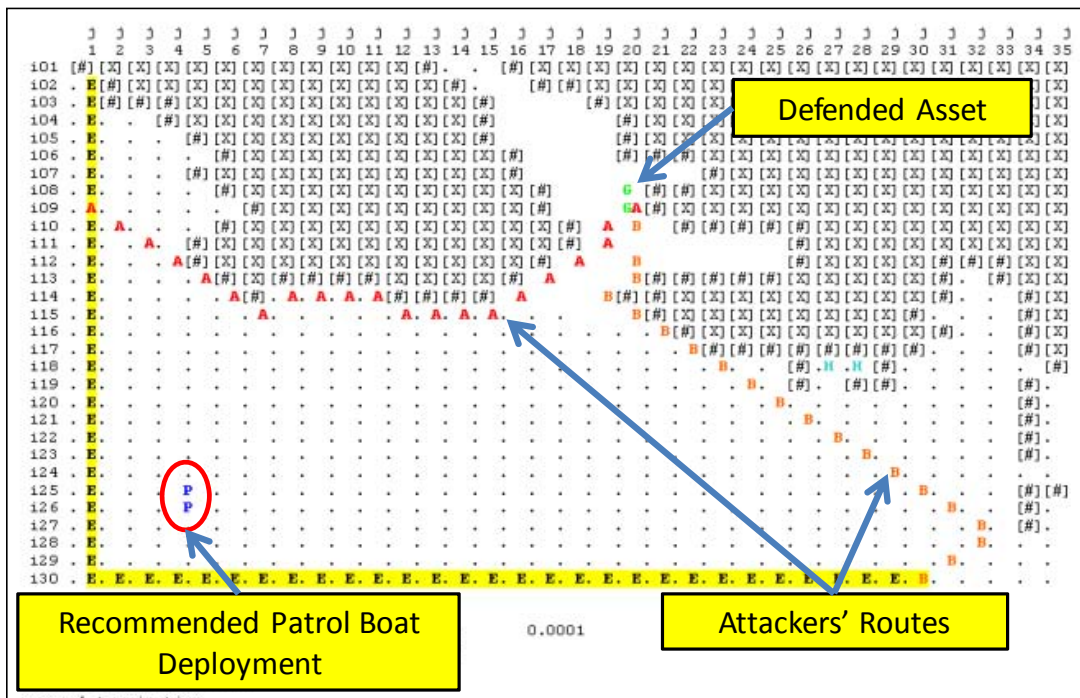
Figure 5.　2 Defenders Against 2 Attackers in HK (After Abdul-Ghaffar, 2008)
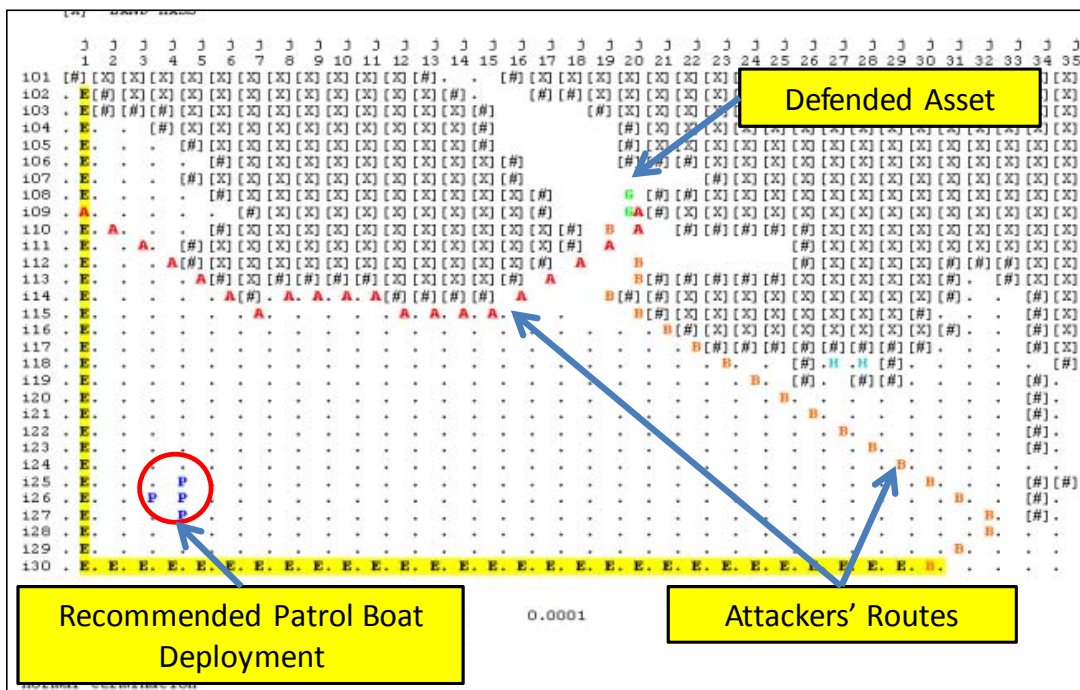
Figure 6.　4 Defenders Against 2 Attackers in HK (After Abdul-Ghaffar, 2008)

7

E.   IMPLICATIONS OF THE FINDINGS

Adul-Ghaffar's objective was to station patrol boats as floating radar picket stations to best detect small vessels while at the same time solving for the best way for threat vessels to approach their target given they know the location of the patrol boats.

He stresses in his conclusions the need to also solve for locating patrol boats for interception. A patrol boat is typically tasked to patrol a sector and performs inspections of ships or shore facilities. In addition, establishing patrol sectors as near as possible to the threat axis or in restricted approach lanes would be considered a prudent tactic to enhance the opportunity for interception. Thus, alternative defensive deployment tactics for patrol boats to be mobile and operate over a larger region will be explored in this thesis, vice stationary solutions for Abdul-Ghaffar's picket boats optimized for detection.

An observation on Abdul-Ghaffar's results were multiple attackers selecting the same route (to minimize the detection probability in a bid to evade the defender), suggesting the employment of a saturation attack tactic. Furthermore, it is plausible that the attacker may choose an alternative deception tactic by diverting the defenders' attention before committing the actual attack. Such variations in attacker tactics could be a concern when stationing patrol boats for intercept, and are explored in this thesis.

F.   DEEPER DISCUSSION

1.   Deployment Position

In an attempt to replicate Abdul-Ghaffar's results, the LA scenario was re-run, and a new optimal deployment was recommended and reproduced in Figure 7. The defenders are now stationed along the path of the attackers, different from the positions that Abdul-Ghaffar had showed previously. This deployment also yields a 100% probability of detection, an indication that more than one optimal (or near optimal) solution might exist for the deployment positions.
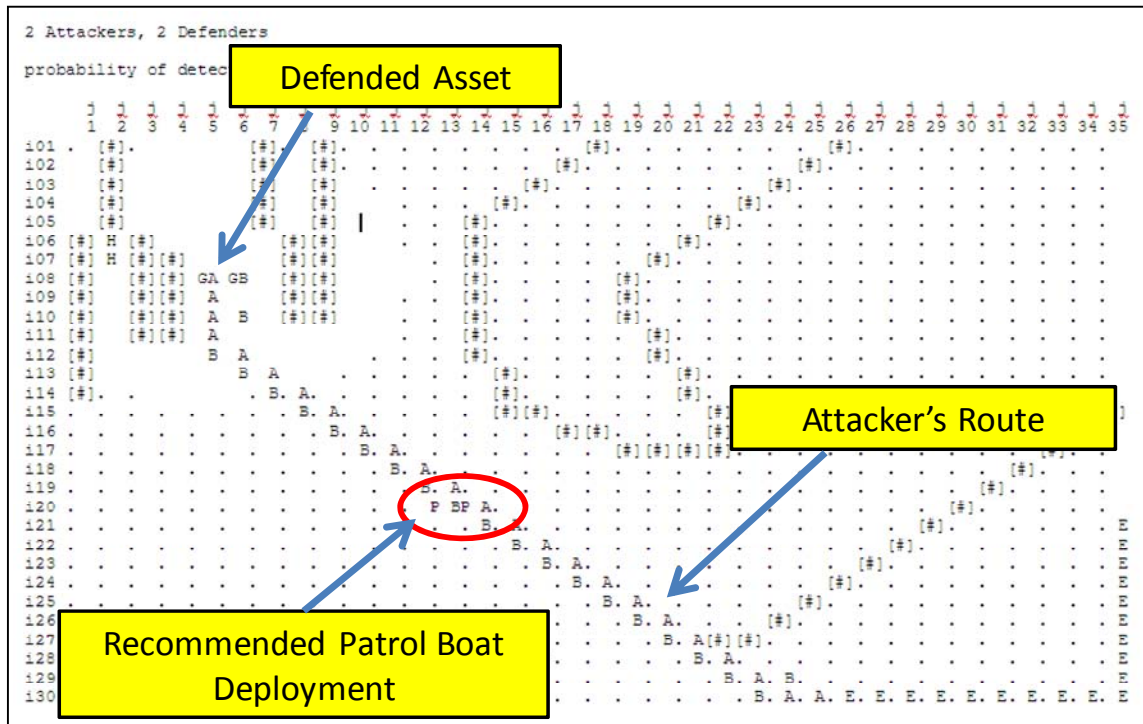
Figure 7.   A Re-run of Abdul-Ghaffar's LA Model for 2 Defenders Against 2 Attackers Showing an Alternative Recommended Deployment for the Patrol Boats

2.   Probability of Detection

The effective radar horizon (Skolnik, 2002, summarized in Figure 8) of the SAFE Defender was found to be 6 nautical miles (NM) for a radar at a height of 6 feet to detect a target 6 feet tall, significantly smaller than the radar range of 36 NM used by Abdul-Ghaffar, and could explain the high probabilities of detection shown in his results.

$$d(nm) = 1.23\left(\sqrt{h_a(ft)} + \sqrt{h_t(ft)}\right)$$

Where:
d: Radar Horizon in Nautical Miles
h_a: Antenna Height
h_t: Target Height

Figure 8.   Radar Horizon Calculation (in Nautical Miles)

With the range of the radar being significantly larger than the area of operations, which is 5 NM wide, Abdul-Ghaffar's cell-to-cell probability of detection of the attacker by the defender's radar was found to be very high (almost 98% probability per cell), such that just two cell-to-cell transitions would yield a high probability of detection of 0.999 (see Figure 9). In effect, as long as the defenders are placed with an unobstructed line of sight to the entrance, there would be a near 100% probability of detection, even for a single defender, explaining Abdul-Ghaffar's results of high probability of detection of the attackers throughout all the four ports that were analyzed.
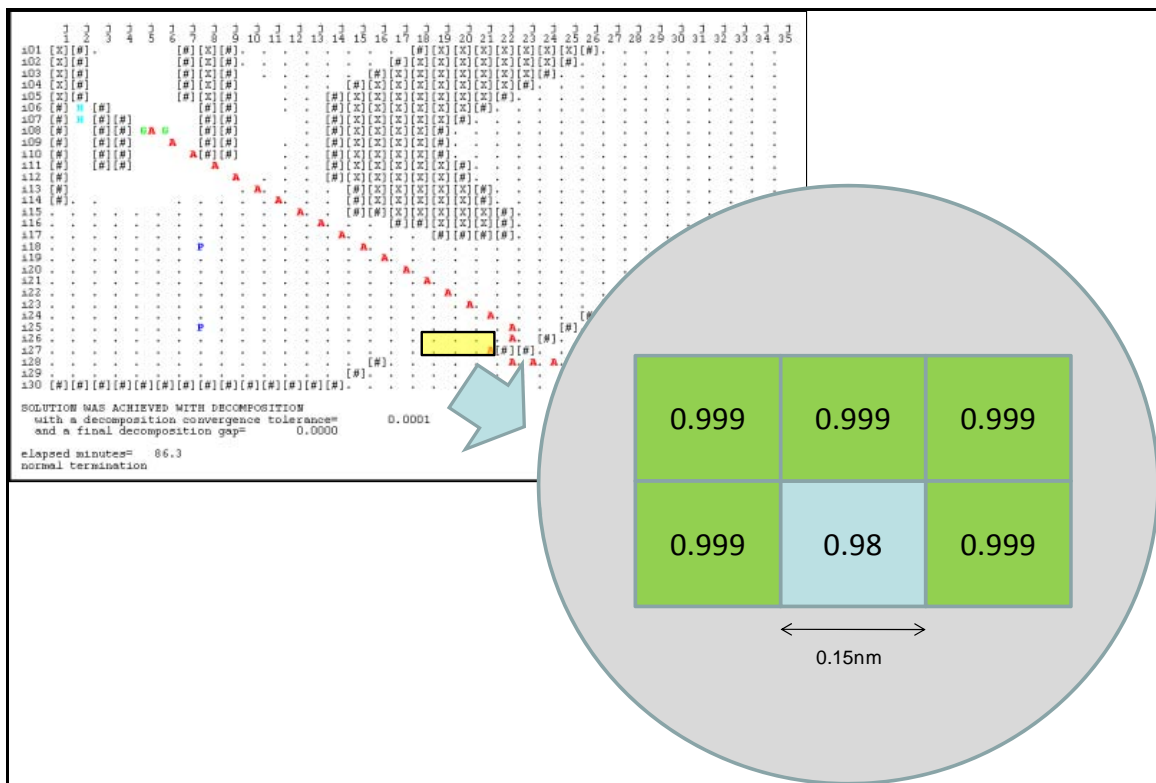
Figure 9.   Detection Probabilities upon Cell Transition

G.   MOTIVATION

Precipitated by an agreement with Abdul-Ghaffar's proposition that the interception of detected small speed-boats with a speed advantage poses "a vexing defense problem" (Abdul-Ghaffar, 2008, p. xviii), and that in reality, there is a possibility

that the attackers and defenders may choose to employ alternative tactics, a need to study the issue of interception of small vessels in greater detail arose.

Detection without interdiction would have negligible impact on actually preventing such a terrorist attack, so this study aims to seek operational insights for defense against small boat attacks by exploring the effectiveness of a range of defensive tactics in interdicting a variety of small boat attack tactics.

Compared to mathematical models, simulation models typically require minimal assumptions about the nature of the problem. MANA (Map Aware Non-uniform Automata, 2007) is a simulation tool for scenario exploration that has been previously employed to study the maritime protection of critical infrastructure assets (Tiburcio, 2005) and naval tactics in an island complex (Lalis, 2007). MANA is a stochastic, time-stepped, agent-based distillation with a quick set-up time and modeling flexibility, having pre-built components to model tactics and simple behaviors such as following waypoints, acting on situational awareness, and avoiding the enemy. Simulation through MANA is chosen to allow more realism in analyzing the engagement between the patrol boats and the attacking speedboats.

The two Measures of Effectiveness (MOEs) driving the analysis are:

1. Probability of attacker success, where a success is defined as at least one attacker reaching the defended asset, and
2. Number of attackers killed.

THIS PAGE INTENTIONALLY LEFT BLANK

III. DETAILED SCENARIO AND MODELING

A. SCENARIO AND MAPS

1. Current Security Strategies to Determine Intent

The difficulty of tracking small vessels was vocalized in the DHS Small Vessel Security Strategy:

> Small vessels may easily blend or disappear into other vessel traffic in ports and the coastal maritime environment, and are usually subject to less scrutiny than larger vessels in these areas. They are often inconspicuous, fast, highly maneuverable, and able to quickly relocate via roads and surface transportation…. (DHS SVSS, 2008, p. 12)

While tracking a small vessel is challenging, it is even more difficult to identify a vessel driven by terrorists with malicious intent among a plethora of innocent boats. Port authorities have implemented varying measures to address these concerns, and facilitate the identification of suspicious vessel behavior.

In the Port of Los Angeles, Controlled Navigation Areas (CNAs) are special zones that prohibit the general boating public and allow only select vessels to approach, "enabling the Port Police to quickly identify vessels that represent anomalies and therefore possible threats to the port" (Port of Los Angeles, 2010, see Figure 10). Unauthorized vessels that approach the CNAs draw immediate attention to themselves, and for the modeling purposes of this study, will be intercepted and investigated by patrol boats.
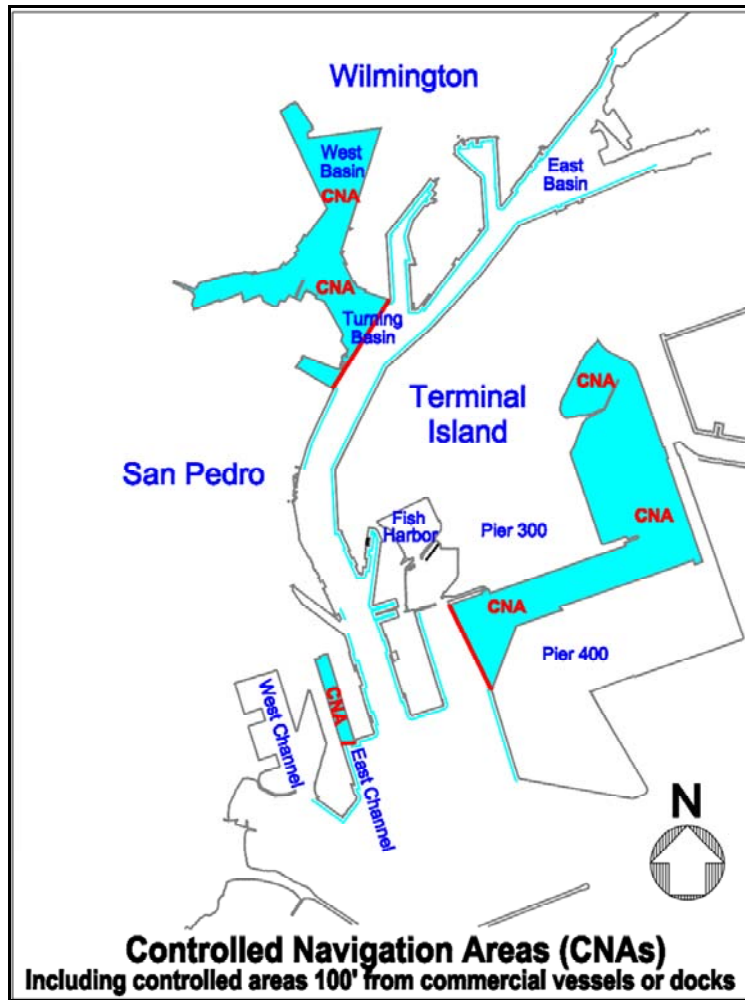
Figure 10.   Controlled Navigation Areas (Port of Los Angeles)

In the Port of Hong Kong, traffic control measures such as traffic separation schemes and speed restrictions exist (see Figure 11). For the purpose of comparison in this study, a security measure is applied on the port, such that only cargo vessels approaching the terminal are allowed to use channel A. Small vessels, such as the attacker speedboats modeled in this study, that deviate from the traffic lane are deemed suspicious and will be investigated.
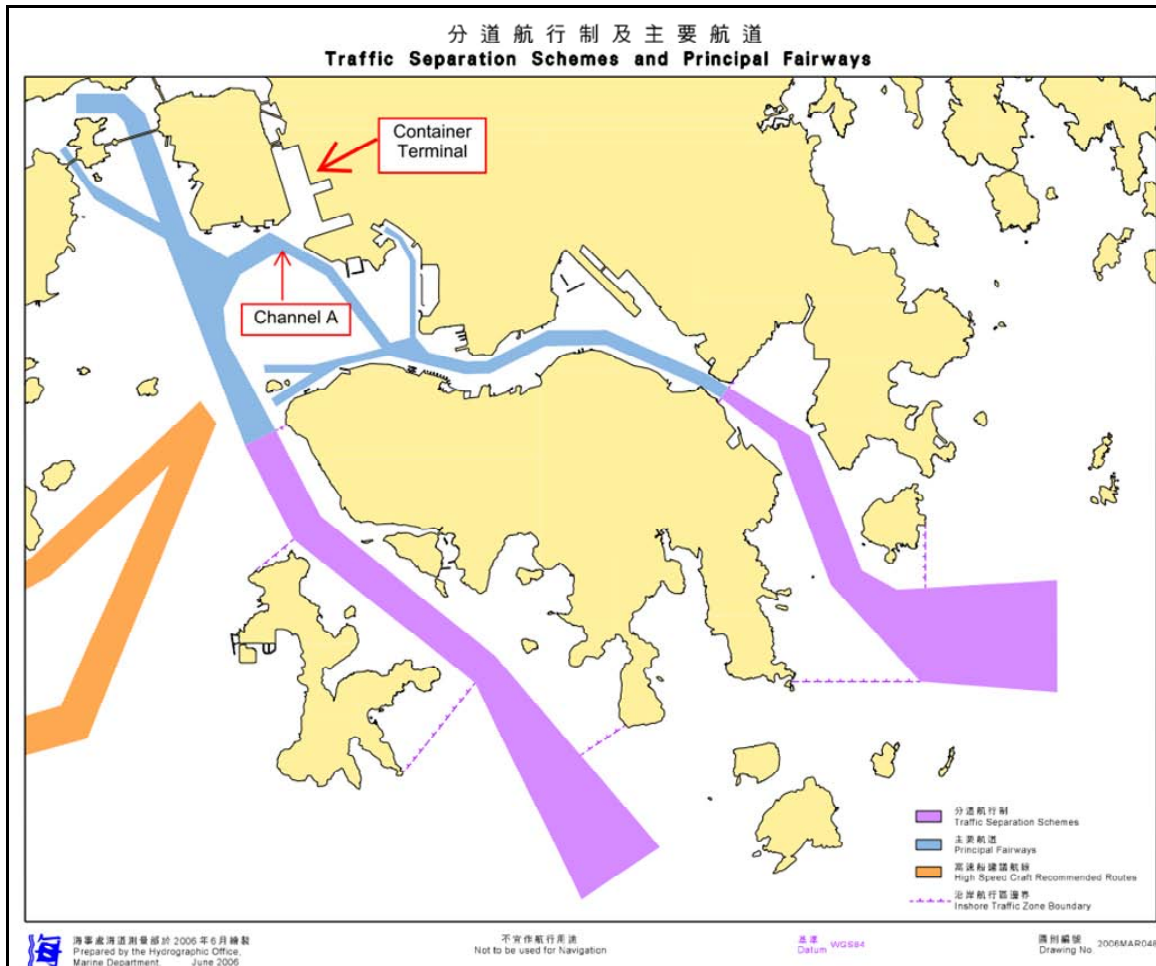
Figure 11.   Traffic Separation Scheme in the Port of Hong Kong (Port of Hong Kong Development Council, after Microsoft Word)

Many major ports perform active surveillance of their waterways via coastal radar and waterside cameras to monitor traffic and prevent ship-to-ship collisions. These assets can also be used to watch for vessels not adhering to the exclusion zones and traffic separation schemes, enabling detection of anomalous behavior of vessels that could possibly indicate malicious intent. Together with the security strategies discussed above, active surveillance is able to build up situational awareness, and this study assumes it will be possible to deduce and identify small vessels that are exhibiting anomalous behavior. In order to determine if the anomalies are malicious, patrol boats will be alerted to intercept and investigate the flagged anomalous vessels.

B. THREAT DEFINITION

1. Possible Attacker Modus Operandi

The attacker is intelligent, and will plan to use a range of tactics in a bid to overcome the defense:

1. **Saturation attack:** Being able to observe the defender, the attacker plots an attack using numerical superiority to overwhelm the defense.

2. **Diversionary attack:** One attacker deliberately behaves in a way to attract the defender's attention (could be entering an exclusion zone, or starting a fire on-board the vessel), while others exploit the gap in the defense and rush in to their objective.

2. Threat as Modeled in MANA

Two distinct squads were created in MANA to represent the saturated attack and diversionary tactic. The attack route the squads take are shown in the maps in Figure 12 for LA and in Figure 13 for HK. For the MANA scenarios with the diversionary attack, the decoy takes the route as indicated on the maps in an attempt to lure the defenders away before the actual attackers begin their attack. The speeds of the attackers are fixed at 54 knots, as they were in Abdul-Ghaffar's study (Abdul-Ghaffar, 2008, p. 9).

Figure 12.　Scenario Setup for LA, Showing Defended Asset and Attackers' Route
(Google Earth, after Microsoft Word)
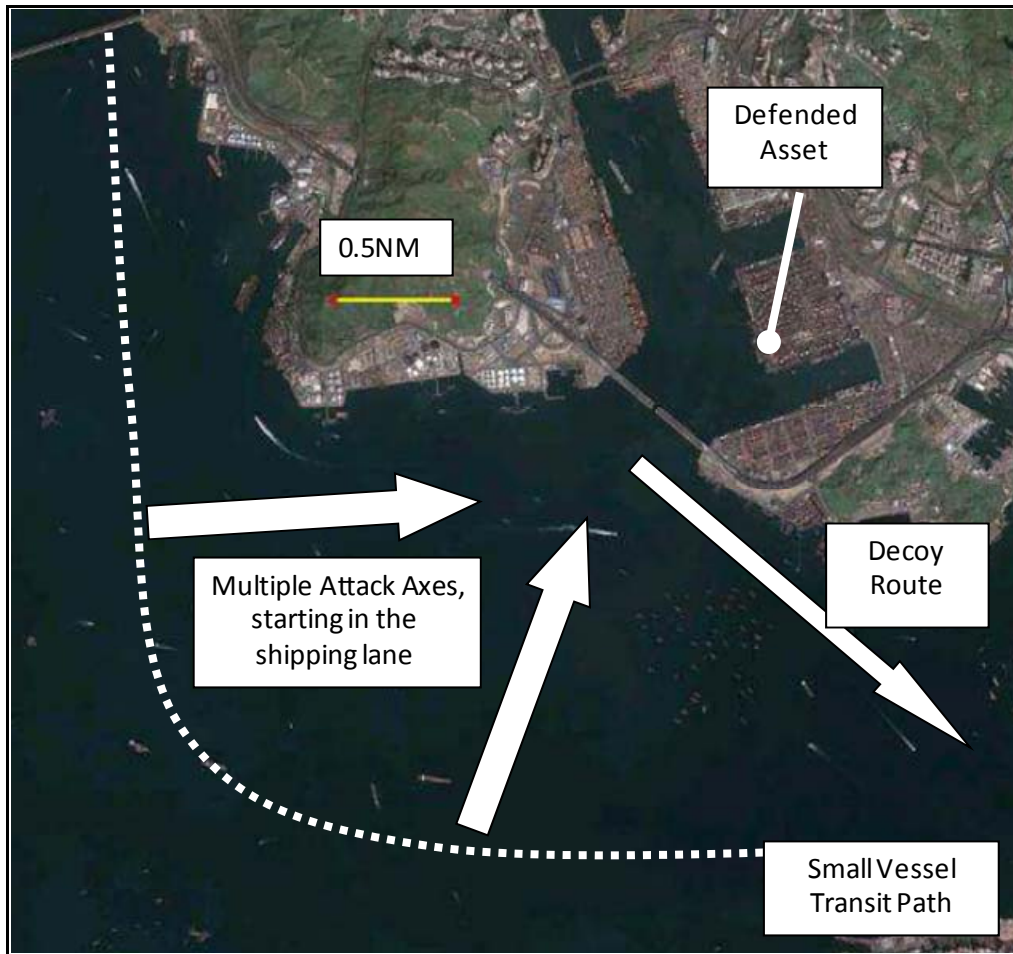
Figure 13.   Scenario Setup for HK, Showing Defended Asset and Attackers' Route
(Google Earth, after Microsoft Word)

C.   DEFENDER CONOPS

1.   Possible Defender Response Tactics

There are three possible defensive postures considered in this study:

1.   **Scramble from Base**: A patrol boat is scrambled from a base at shore near the defended asset to intercept the intruder. It is assumed (as was in Abdul-Ghaffar's study) that there is only one defended asset. A downside is that there will be a time-lag for the operators to start the engines and get to the intercept point.

2.   **Barrier Patrol:** A standard barrier patrol is assigned a stretch of water to patrol, and acts to deter and detect intruders. The barrier can be positioned across the mouth of a channel perpendicular to the axis of the anticipated attack. The advantage of this mode of deployment compared to scrambling from base is that the patrol boats' engines are already hot and ready to give chase to any intruder, but the downside to the barrier patrol is that the patrol boat may take time to turn and join the chase, and a predictable patrol route can be easily observed by the attacker. The attacker will have opportunity to observe and wait for the patrol boat to pass before making an attempt to break through the barrier, giving the defender a slight disadvantage due to its orientation.

3.   **Random Patrol:** A patrol boat is assigned responsibility for a given sector. The patrol can randomly choose to approach passing ships in a channel, or go closer to shore to inspect facilities, or stay within the channel like a barrier patrol. This randomness reduces the predictability of the patrol boat's location, hopefully making it more difficult for the attacker to seize an opportunity to strike when the patrol boat is in a disadvantaged position.

A MANA squad is created for each of the defender tactics, with their deployments and patrol routes shown in Figures 14 and 15 for the Port of Los Angeles and the Port of Hong Kong respectively. The patrol boats at these deployment positions satisfy the condition of having line of sight to the attackers' axes of approach, yielding a 100% probability of detection, as in discussed in Chapter II.

Figure 14.   Scenario Setup for LA, Showing Defenders' Deployment and Patrol Routes
(After Google Earth)
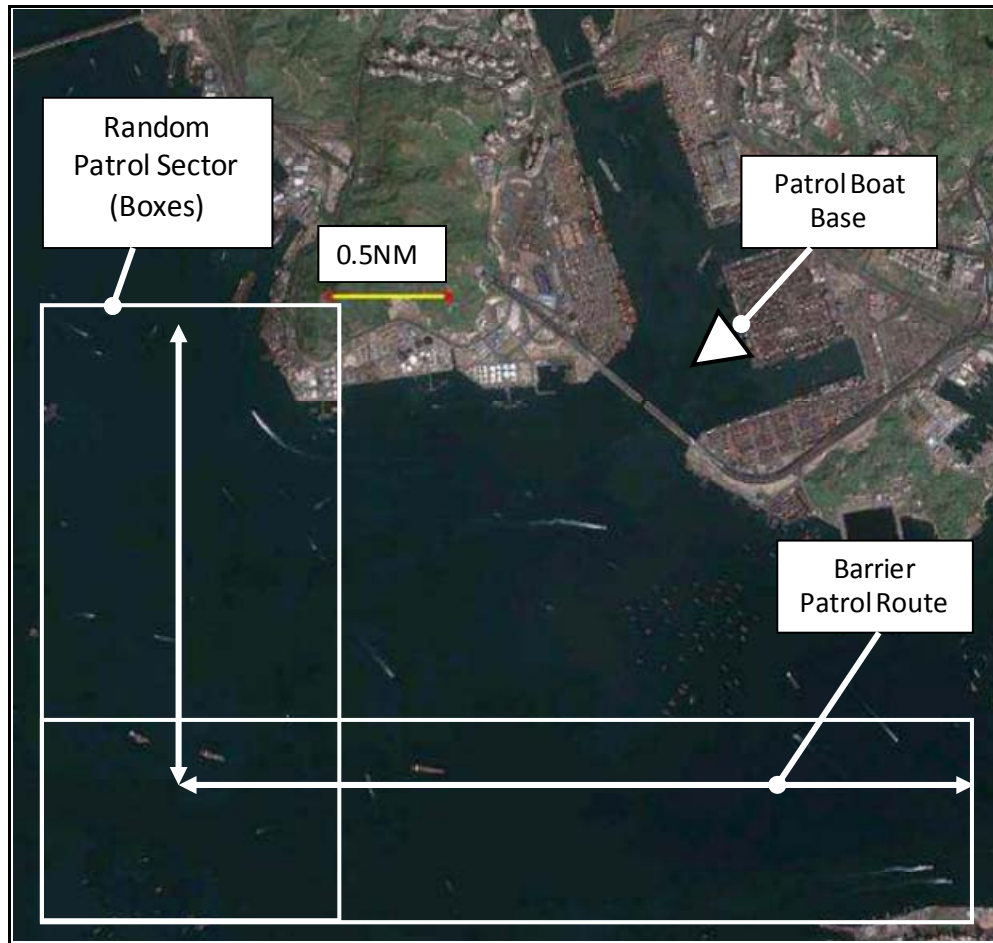
Figure 15.   Scenario Setup for HK, Showing Defenders' Deployment and Patrol Routes
(After Google Earth)

2.   Rules of Engagement

The interception engagement can be broken down into three stages:

i)   **Determine intent of the vessel**: Once the patrol boat has been alerted, it
will vector toward the intruder to interdict and hail the approaching vessel,
with the objective to warn the vessel that it has infringed upon the
exclusion zone.

ii)   **Deter the vessel**: If the intruding vessel, after having been warned,
continues its course, it will be taken that it has malicious intent and
attempts will be made to deter the crew from their current path with non-
lethal weapons (if the patrol boat is equipped).

iii)   **Stop the vessel**: Should the non-lethal weapons fail to turn the vessel back, effort must be made to stop the intruder. This could be achieved either by the patrol boats' gunnery or by ramming the intruder.

In the simulation model, however, only a real threat intrudes (there are no false alarms) so the patrol boat always seeks to stop the intruding vessel and only step (iii) is modeled.

3.   Kinematic Analysis of Interception

The interception of small boats bears close resemblance to the interception of aircraft attacking a ship (Naval Operations Analysis, 1999). In order to conduct a successful intercept, the patrol boat must close in on the attacker boat to within weapon engagement range. The geometry of the engagement is shown in Figure 16, with successful interceptions occurring for combinations of Closest Point of Approach (CPA) and Range at Detection (R_{Det}) for which θ_A has valid solutions. This equation was used to validate the interception capabilities of the defender patrol boats in MANA.
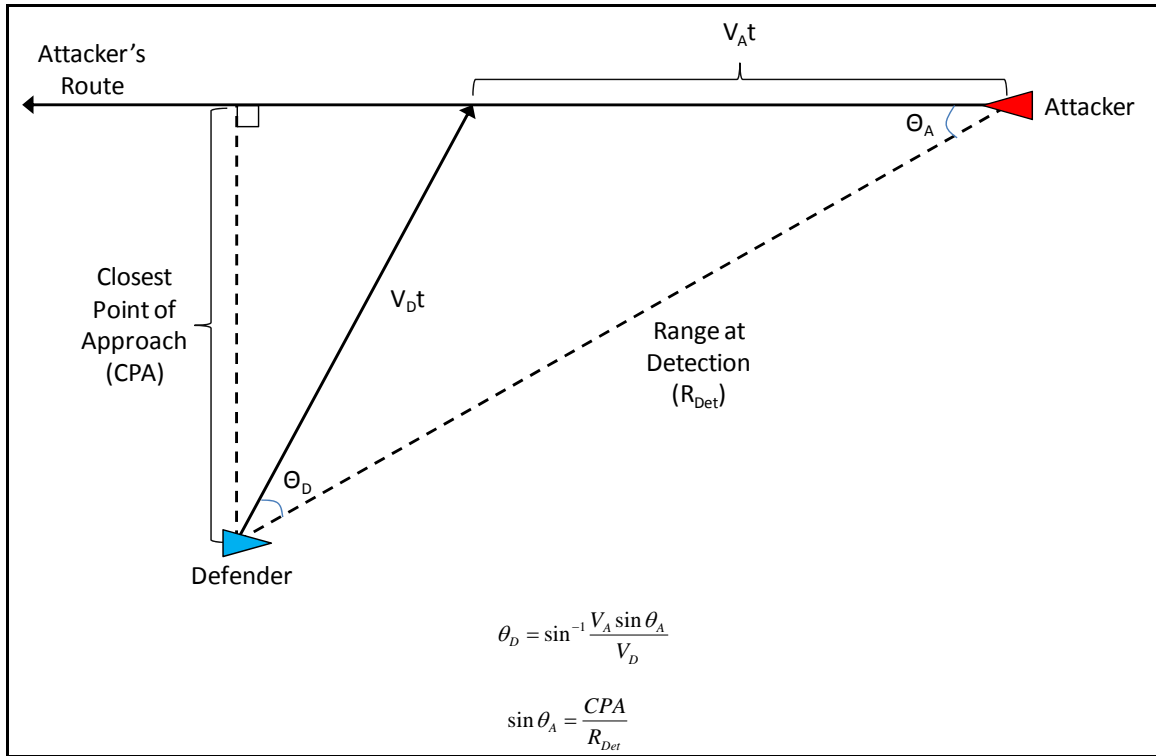
Figure 16.   Geometry of Interception Engagement

22

D. FACTORS AND LEVELS

The scope of this study is to compare the robustness of alternative defensive deployments against variations in the attackers' tactics, focusing on the key factors of current security strategy policies and current platforms. The controllable and noise (non-controllable) factors that are involved in the real scenario, whether they were considered in this study, and the levels that were studied, are given in Tables 1 and 2 respectively.

While it is beyond the scope of this thesis, it is possible for future research on variables that were fixed in this study to quantify their effect on interception operations. Alternative defender and attacker platforms could be contrasted, or the effect of shipping density analyzed. High shipping density in a channel would greatly restrict the maneuver space for a patrol boat attempting the interception of a speedboat that is weaving its way between slower cargo ships, reducing the effectiveness of the defense. Simulation could also be used to analyze the variation of sensor performances, environmental conditions, or operator skill levels.

Controllable Factors		Fixed / Variable	Levels
Security Policy		Fixed	Coastal surveillance with controlled navigation
Defender	Tactics	Variable	3 levels: Static, Barrier patrol, Random Patrol
	Platform	Fixed	SAFE Defender class patrol boat
	Number	Variable	1 to 4
	Speed	Fixed	45 knots
	Weapons	Fixed	12.7 mm (0.5 in) gun

Table 1.   Controllable Analysis Factors

Non-controllable Factors		Fixed / Variable	Levels
Environ-mental	Weather	Fixed	Fair weather
	Sea-State	Fixed	Benign (0 to 1)
	Shipping Density	Not Analyzed	
Attacker	Tactics	Variable	2 levels: Saturation and Diversionary
	Platform	Fixed	Baja Outlaw 20' speedboat
	Number	Variable	Saturation: 1 to 4 Diversionary: 1 decoy and 1 to 3 actual attackers
	Speed	Fixed	54 knots

Table 2.   Non-controllable Analysis Factors

E.   DESIGN OF EXPERIMENT

The first experiment uses the deployment positions as recommended by Abdul-Ghaffar's study, but with the probability of at least one attacker reaching the defended asset instead of the probability of detection as the MOE. The number of attackers was varied between one to four, as was the number of defenders, for a total of 16 design points, with 100 simulation replications per design point for this baseline case.

Subsequent experiments were performed to compare the effectiveness of the three defender tactics against the two attacker tactics. In view of the relatively small number of factor levels, a full factorial experimental design (see Table 3) was chosen to survey the entire parameter space for the two factors of attacker and defender tactics, with their respective number of platforms, for a total of 84 design points, with 100 replications for each design point. Each replication took approximately 30 seconds to run.

MOE 1: Prob (At least 1 attacker succeeds)			Red Tactics						
MOE 2: Number of Attackers Killed			Saturation				Diversionary		
		Num of	Number of Attackers				Number of Attackers		
		Defenders	1	2	3	4	1	2	3
Blue Tactics	Static	1							
		2							
		3							
		4							
	Barrier	1							
		2							
		3							
		4							
	Random	1							
		2							
		3							
		4							

Table 3.   Run Matrix for the Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RESULTS AND ANALYSIS

A. BASELINE SCENARIO (LA)

1. Defense Against One Attacker

The results of the baseline scenario replicating Abdul-Ghaffar's recommended patrol boat deployment positions are presented in Figure 17. The vertical axis shows the response variable "Red_Success," an indicator variable where 1 indicates at least one attacker evaded and outran the defenders and made it to their target, while 0 indicates all attackers were stopped by the defenders. Values between 0 and 1 indicate the proportion of the 100 replications in which at least one attacker reaches its goal. The top horizontal axis breaks the chart into four columns, such that the left-most column shows the performance of one to four defenders against one attacker. Columns two to four show the performance against two to four attackers, respectively. When there is one defender against one attacker, a Red_Success rate of 5% shows that interdiction is successful 95% of the time, improving to 100% when there is more than one defender. (Note that for 100 replications, the standard error associated with these empirical findings is $10\sqrt{(pq)} \leq 5$, where p is the true proportion of success.)
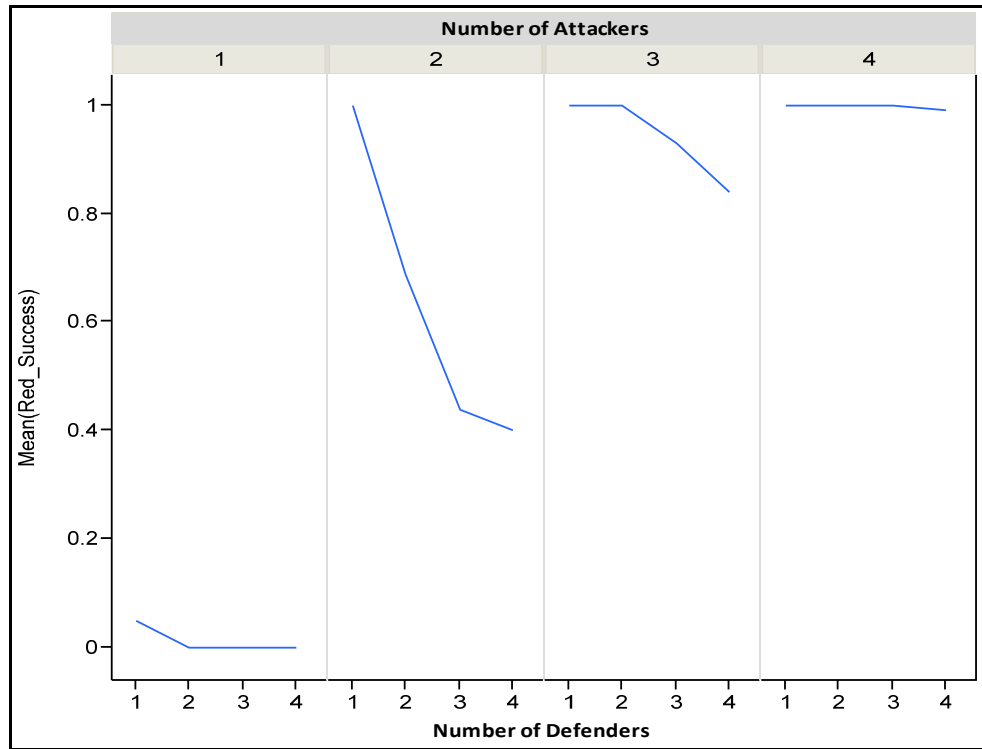
Figure 17.   Probability of Attacker Success, Grouped by Number of Attackers

Based on the kinematic analysis provided in Chapter III, the geometry between the attacker and defender in the given deployment position should be able to guarantee an interdiction all the time. However, in the 5% of simulation runs where the attacker manages to reach its intended target, the defender is unable to intercept the attacker. This is partially due to the limitation of MANA agents in thinking ahead to intelligently plan and move on an intercept course.

Acknowledging this as a limitation in modeling the engagement, the real world equivalent of engagements between two moving boats is also fraught with uncertainties. Firstly, in practice, the defender may not know for certain the attacker's goal to be able to anticipate the heading. In addition, when the defender approaches sufficiently close to fire upon the attacker, there is no guarantee a gun round will be able to hit the attacker due to the motion of the boat going over the waves, who is also in a moving boat on the waves. With the instability of the firing platform, it is very possible that bullets can hit the attacker's boat but not injure the attacker, or miss the boat altogether. Moreover, at high speeds of 40 knots, distances close very fast and the defender may overshoot the

attacker, who is also attempting to evade the defender by maneuvering, ending up in a tail-chase with the attacker being able to outrun the defender. These factors will result in a failed interception, even though the defender may be able to approach sufficiently close to the attacker.

Given the complexity and uncertainty of the engagement in the real world, it is highly probable that the results shown in this analysis are overly optimistic. Nevertheless, the model serves as a common yardstick to gauge the effectiveness of the defender in each scenario and perform a comparative analysis between the tactics, and draw insights into the issues concerning defense against small boat attacks.

2.   Defense Against Two Attackers

In the second column of Figure 17, a dramatic drop in the defender's effectiveness is observed when there are now two attackers. If there is only one defender, only one attacker will typically be interdicted, and the other will successfully reach the intended target, explaining the 100% Red_Success rate. The defender is outnumbered and is only able to focus the interception effort on one attacker. When there are two defenders, the attackers succeed 69% of the time, with only 31% chance that both the attackers will be stopped. More defenders perform better, reducing the proportion of attacker success to 44% with three defenders, and 40% with four defenders.

The number of attackers intercepted in an engagement is shown on the left vertical axis of Figure 18. The grouping by number of attackers on the top horizontal axis breaks the chart into four columns, with the left-most column showing the performance of one to four defenders against one attacker. The right axis splits the chart into two rows, with the top row showing the number of attackers intercepted for runs where Red_Success is 0, while the bottom half shows the average number of attackers intercepted on the runs where at least one attacker reached the defended asset.
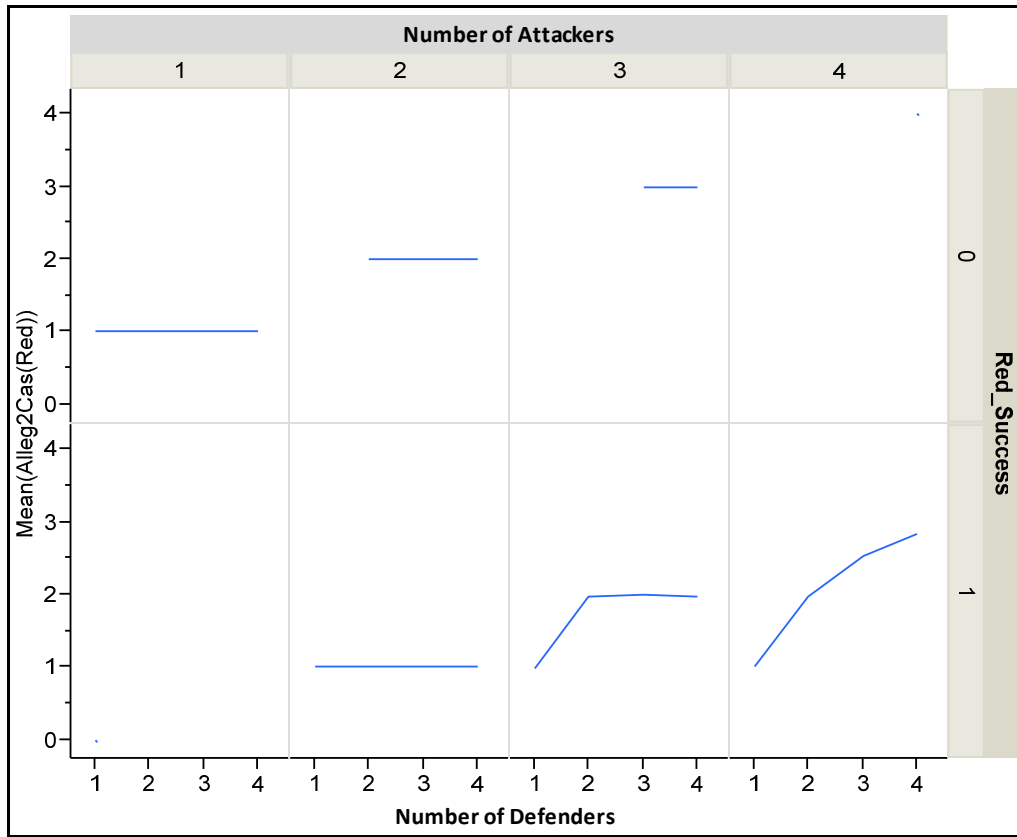
Figure 18.　Number of Attackers Intercepted, Grouped by Number of Attackers and Red_Success

When two defenders and two attackers engage (results reflected in the bottom row of the second column of Figure 18), often times only one attacker is intercepted leading to the attackers' high probability of success of 69%. A more concerning result is that when four defenders engage two attackers, there is still a high chance that only one attacker is intercepted and the other attacker is able to evade and conduct a successful attack.

This result reflects the situation in a real engagement when two defenders give chase to a single attacker, in the hope of applying numerical superiority to obtain a higher chance of stopping the attacker. Since both defenders focus on one attacker, the other attacker manages to slip past and score its' objective. It is also conceivable that due to the fast-paced chase, there would be confusion regarding which attacker each patrol boat is to focus on. This modeling limitation may be less evident in practice, if good command and control is able to reduce the confusion.

The inability to completely prevent an attack when there are just two attackers is a cause for concern, especially when the defender has the numerical advantage (three or four defenders, see bottom row of second column of Figure 18). It is often thought that the side with a numerical advantage has the higher odds of winning, but due to the difficulties of the engagement of a fast-moving target on the seas and high speeds, complicated by the confusion during the engagement, there is opportunity for the attacker to break through the defenses and commit a successful attack, nullifying any numerical advantage the defender may have.

3. Defense Against Three and Four Attackers

The defenders have a hard time defending against three simultaneous attacks, mustering an interdiction rate of only 7% with three defenders and 16% with four defenders (see the third column in Figure 17). When there are four attackers (see the fourth column of Figure 17), it is almost impossible to stop all the attackers. The results underscore the difficulties in the engagement due to the unstable firing platform, maneuvering opponents and confusion during the interception mentioned above. The results also highlight a further weakness that can be exploited by the attacker—that having more attackers will distribute the attention of the defenders, elevating the chance of at least one attacker breaking through successfully. This effect will be seen more clearly in the diversionary attack tactic, and further discussed.

B. SATURATION ATTACK AGAINST THE PORT OF LA

1. Scramble Tactic Effectiveness

When the defenders scramble from shore to intercept an incoming threat, if there is one attacker or four attackers, the attack is fended off equally well as the stationary position recommended by Abdul-Ghaffar (see columns one and four in Figure 19). The scramble from shore tactic, however, produces a higher proportion of success when there are two and three attackers.
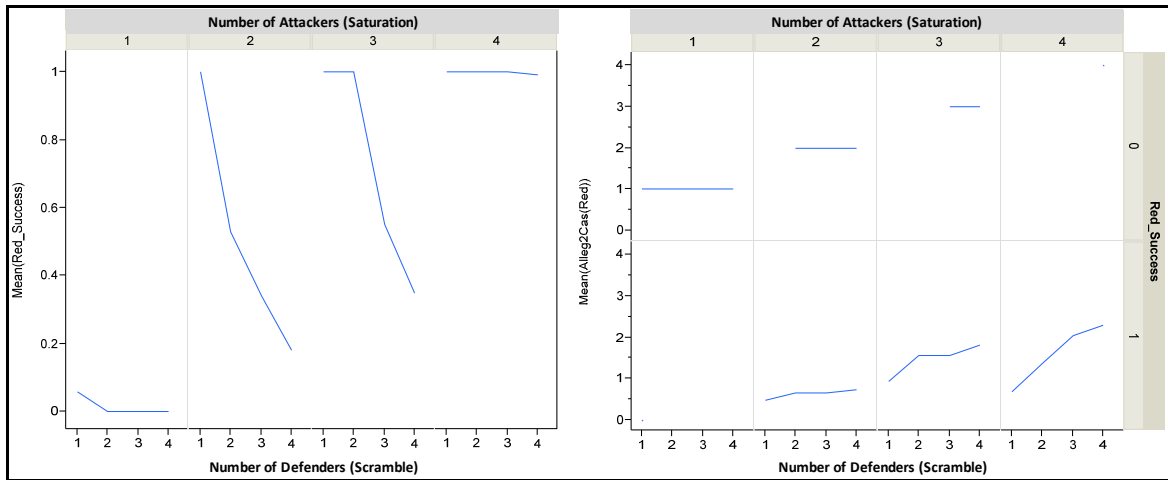
Figure 19.   Effectiveness of Scramble Tactic Against a Saturation Attack (LA)

There is an advantage in scrambling patrol boats from shore to intercept an inbound intruder, since the intruder will be headed straight to where the defenders are, giving rise to a head-on engagement. This can be a better situation than when the patrol boat attempts an intercept that may end up as a tail-chase. Admittedly, the advantage may be limited to the specific engagement geometry between the patrol boats and the attackers considered in the scenario setup. However, the same engagement limitations of shooting a moving boat from a moving boat still exist, and the consequences of a head-to-head collision would be disastrous and lead to the damage or capsizing of either the defender or attacker. Such a collision led to the deaths of two officers in Singapore in 2007 (Wikipedia, *List of Singapore police officers killed in the line of duty*) when a Singapore Police Coast Guard interceptor craft collided with a smuggler's speedboat, resulting in both boats capsizing and trapping the officers within.

2.   Barrier Patrol Effectiveness

A barrier patrol performs worse than the tactic of scrambling from shore. In a one-on-one engagement, the attacker has a 30% success rate in getting through, and more than 70% chance of a successful attack if there are two or more attackers (Figure 20). A reason for the poorer performance is due to the engagement geometry, i.e., the barrier patrol path may have taken the patrol boat too far from the path of the attacker to enable a successful interception.
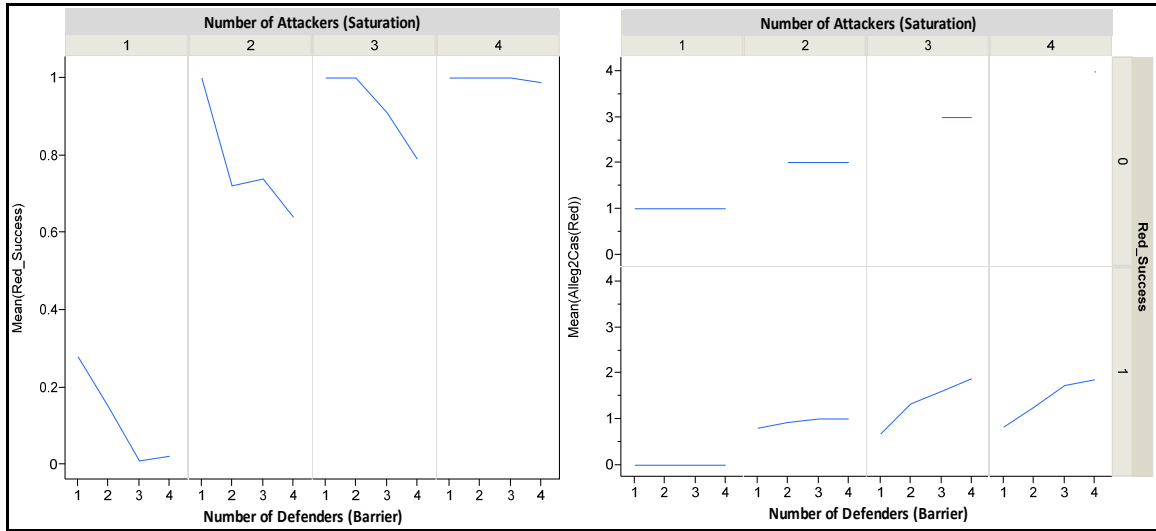
Figure 20.   Effectiveness of Barrier Patrol Against a Saturation Attack (LA)

A real world engagement may be even worse than these results—given the fact that the attacker would be able to observe the position of the patrol boat, and wait for it to travel a distance away before commencing their attack, which will result in a tail chase that disadvantages the defender, who is responding from afar.

3.   Random Patrol Effectiveness

Adding random elements to break the predictability of a barrier patrol does not improve the ability of the defender to stop the attackers in the model. A one-on-one engagement from a random patrol (the left column in Figure 21) fares slightly worse than the regular barrier patrol, letting an attacker through 40% of the time. Against two or more attackers, the results are similar to the barrier patrol. The random patrol has the same weakness that attackers can exploit, namely biding their time until the patrol has passed, despite the randomness of patrol route. All the attacker has to do is to observe one instance of the patrol boat passing by, wait for a few minutes, and execute the attack at full speed, giving the defender a disadvantage for being a distance away.

33
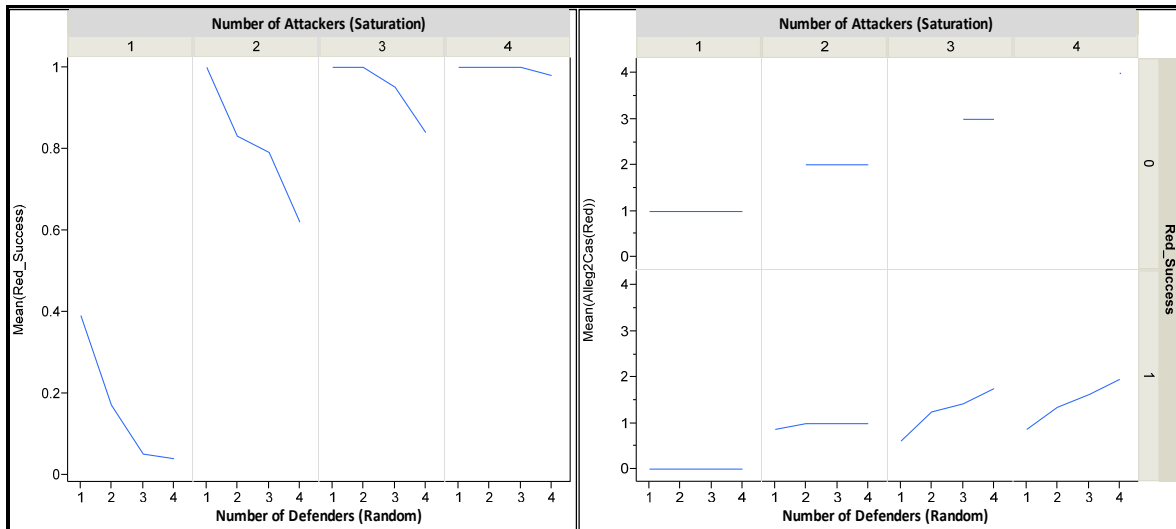
Figure 21. Effectiveness of Random Patrol Against a Saturation Attack (LA)

C. SATURATION ATTACK AGAINST THE PORT OF HK

1. Scramble Tactic Effectiveness

For a one-on-one engagement, the results are consistent with that seen for the Port of Los Angeles, with only 5% of attacks succeeding (Figure 22). When there are two attackers, two defenders are able to stop both attackers 80% of the time for Hong Kong, compared to 50% in Los Angeles. Three defenders are able to reduce three attackers' success rate to 40%, while in the four-on-four engagement, attackers succeed 80% of the time.
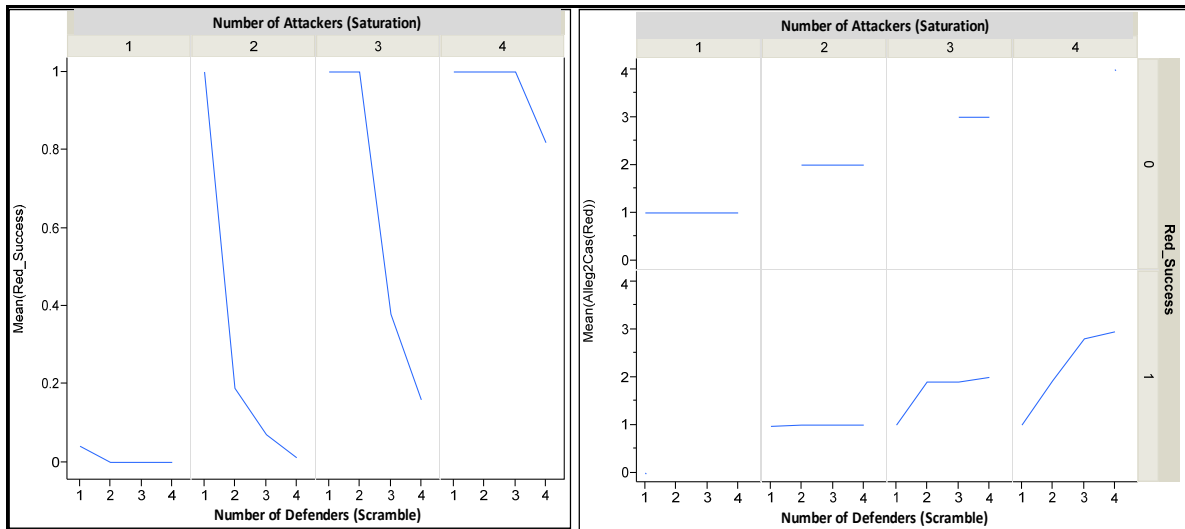
Figure 22.   Effectiveness of Scramble Tactic Against a Saturation Attack (HK)

These results show the same complement of defenders can defend Hong Kong slightly better than Los Angeles. Upon closer analysis, the attackers in LA are constrained to a smaller axis of attack. The defenders are drawn toward the attackers, and when there is more than one attacker, an attacker will be able to break through the defender's lines in the melee, and succeed to strike the target. In the HK scenario, there are more axes for the attackers to spread out, giving opportunity for the defenders to break off from one engagement and intercept the attacker approaching along another axis. This finding, coupled with the previous observation that the defenders' numerical advantage can be nullified in a saturation attack, hints that a simultaneous concentrated single axis attack could be more lethal than if the attackers spread themselves out.

2.   Barrier and Random Patrol Effectiveness

The barrier patrol performs worse than scrambling from base (see Figure 23), consistent with what was observed in LA, since the attackers can wait for the patrol to pass and exploit the engagement geometry to their advantage. The defenders on barrier patrol in HK now perform worse than their counterparts in LA, due to the longer patrol route, favoring the attacker. A similar situation is observed for the random patrol in HK (see Figure 24).
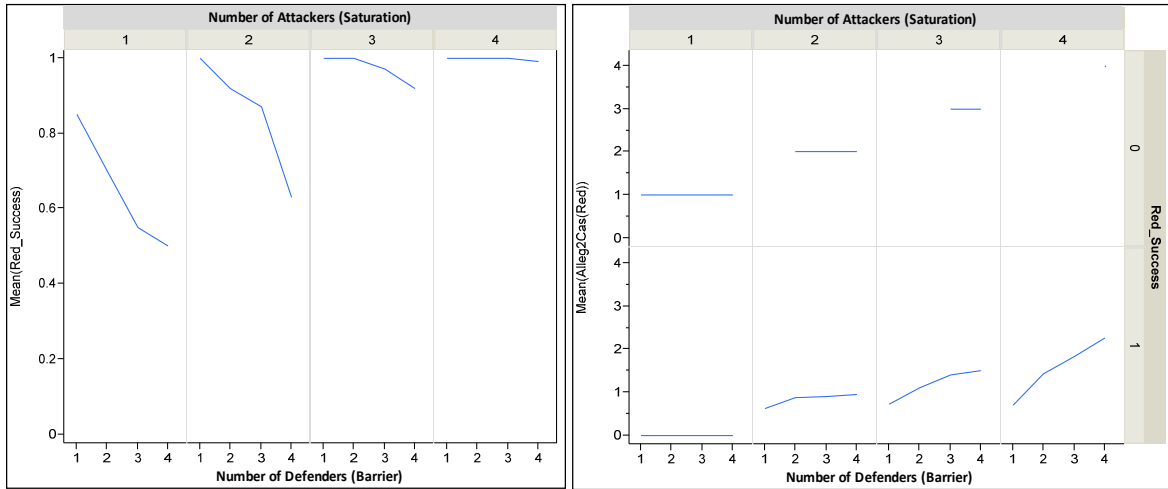
Figure 23.   Effectiveness of Barrier Patrol Against a Saturation Attack (HK)
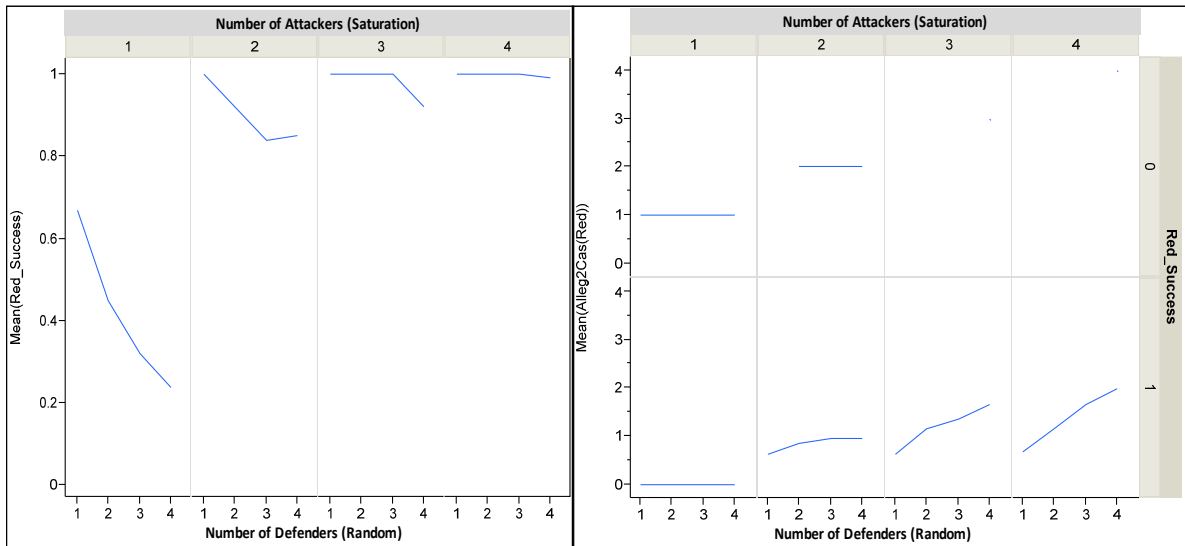
Figure 24.   Random Barrier Against a Saturation Attack (HK)

D.   DIVERSIONARY ATTACK IN THE PORT OF LA

1.   Effectiveness of Response from Static Positions

A diversionary attack is extremely effective in the Port of Los Angeles. None of the defender tactics managed to stop any attack, leading to the dismal results shown in Figure 25. With just one attacker (and the decoy), the terrorists are able to reach their target unopposed. Once the defenders have been drawn away by the decoy, the attackers

36

are able to close the short distance between the traffic lane (where the attackers start) and the target, leaving the defenders no chance of returning to intercept the new intruders.

In the model, all the available defenders were automatically tasked to intercept the decoy, which may make sense if the intruder were a real attacker, since having more interceptors would raise the chances of a successful intercept. In reality it would be possible to be flexible and keep some patrol boats at their current station while sending one or two to intercept the intruder. The results of this study are a cautionary tale on the possibility that the terrorists could use deception to achieve their goals, and the disastrous result if the defender is not ready for such a situation.

E.   DIVERSIONARY ATTACK IN THE PORT OF HK

The results show the defenders are equally inept at protecting the Port of Hong Kong as the Port of Los Angeles, with the attackers succeeding nearly 100% of the time (see Figure 26). There is, however, one surprising finding. The tactic of scrambling from shore against three attackers, and patrolling defenders against two or three attackers, stand a chance of intercepting the attackers.

Due to the distance between the traffic lane and the attacker's goal, the defenders that were already responding to the decoy are able to see and respond to the newer (authentic) attacker some of the time. This explains the slight trend that as the number of attackers and defenders increase, the more likely a successful interception can take place (third column of Figure 26). Unfortunately, there are more attackers than those intercepted, and the attack is still successful since at least one attacker made it past the defenders and executed the attack.
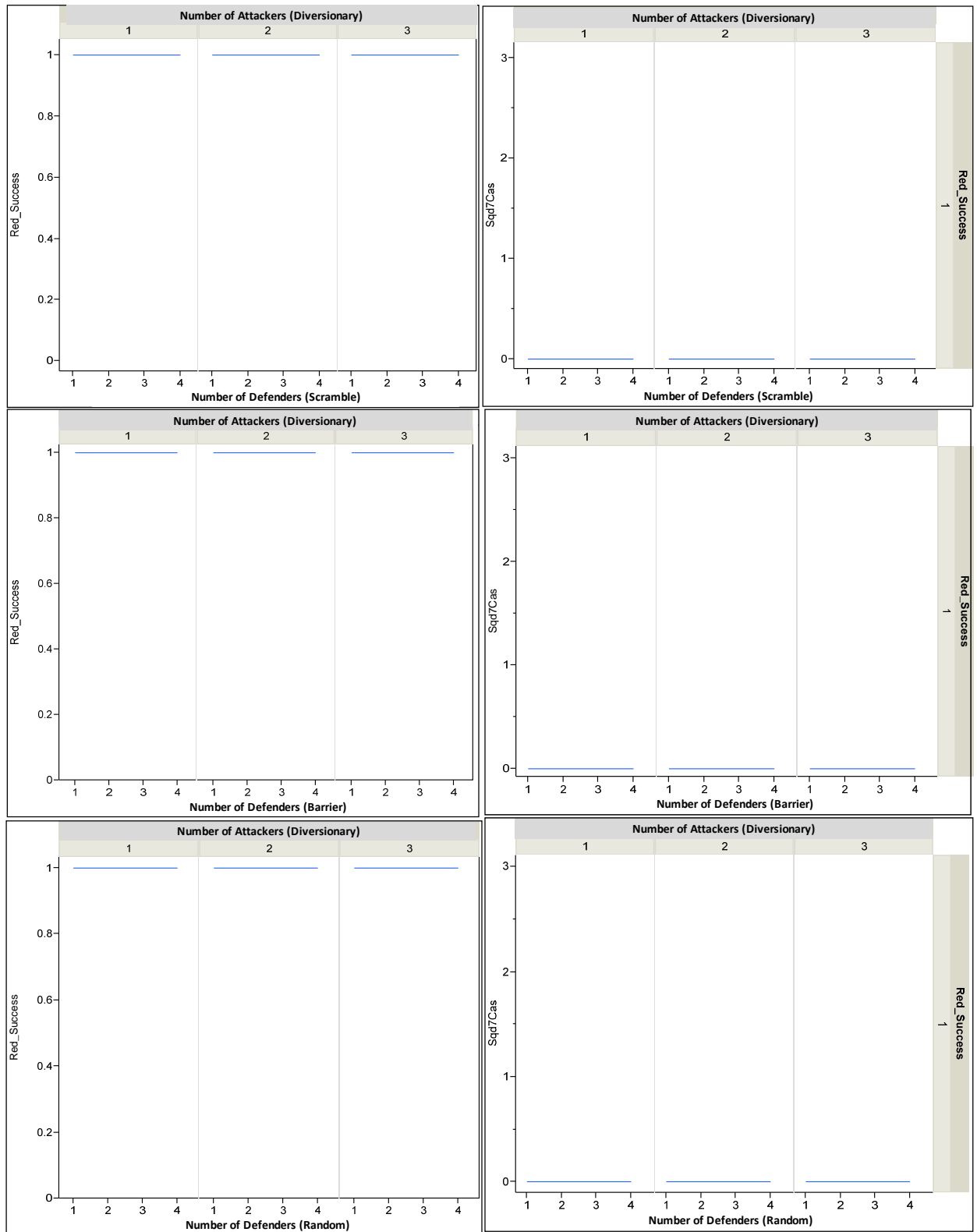
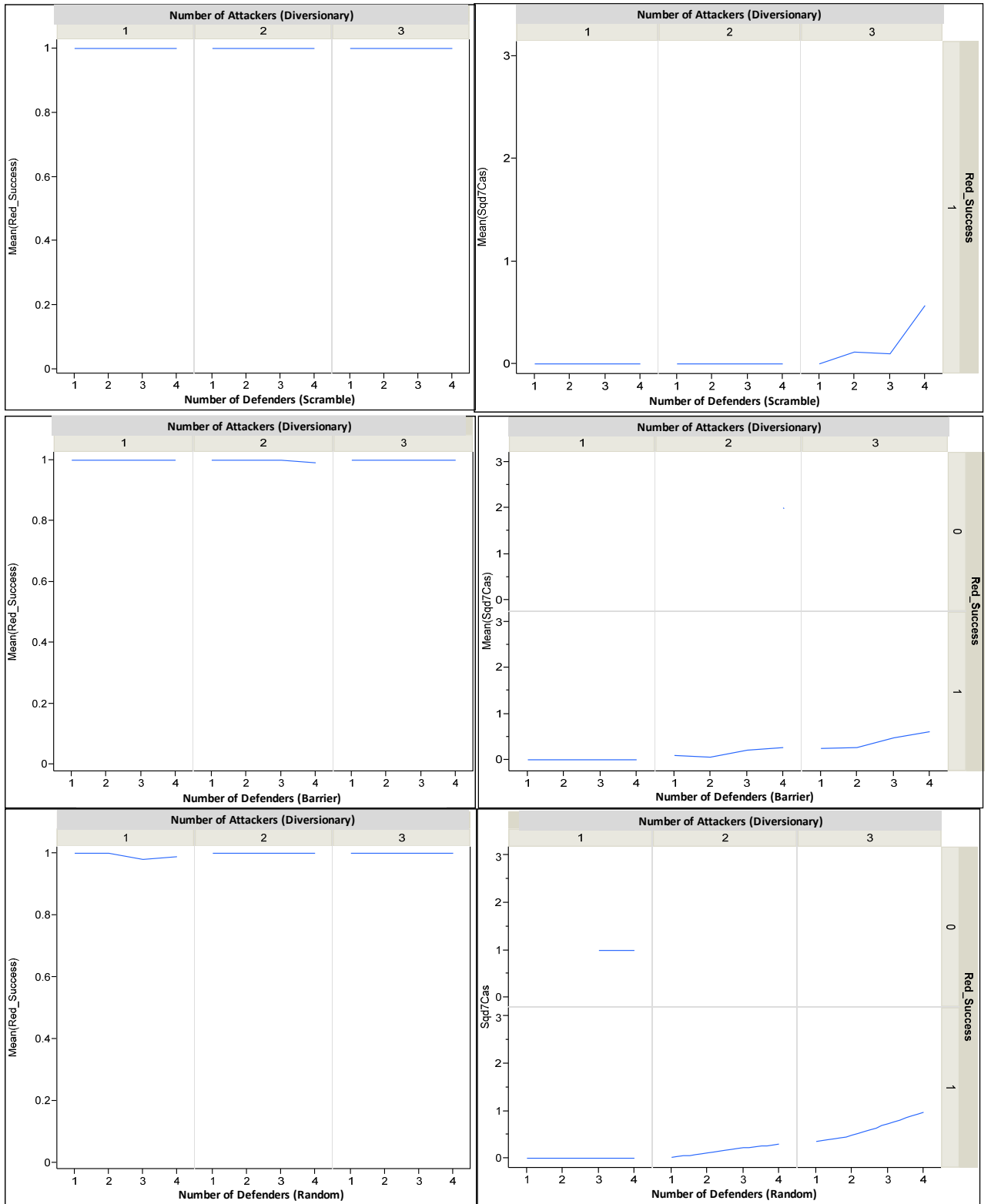Figure 25.   Highly Successful Diversionary Attacks (LA)

Figure 26.   Highly Successful Diversionary Attacks (HK)

THIS PAGE INTENTIONALLY LEFT BLANK

V.   CONCLUSION

A.   OPERATIONAL INSIGHTS

1.   Attacker Tactics

Across the scenarios examined, a diversionary attack is the most effective tactic the attacker can use, promising a near 100% chance of the attack succeeding. It takes just one accomplice boat diverting the defender's attention, while the real attacker boat slips through the compromised defenses and delivers a nasty blow. This highlights a potential weakness in the defender's rules of engagement that the attacker can exploit, and could be mitigated by a refinement of tactics for the contingency of a deception attack, by ensuring that not all defender assets are assigned to intercept the first intruder, but to retain defensive assets for potential follow-on attacks.

The alternative tactic, the saturation attack, utilizing two attack boats against two defenders, or three boats against three or more defenders, proves difficult to defend against, having attack success rates exceeding 50%. This is primarily due to the effect of inaccuracies in shooting while moving and confusion at high speeds during the engagement, and it is a worrisome finding that shows the defender's numerical advantage can be nullified in a deliberate attack with two or more boat attacks simultaneously on a single axis.

2.   Defender Tactics

All the defender tactics considered are glaringly susceptible to deception by a diversionary attack; however, there are some differences between the defender tactics against a saturation attack. Scrambling patrol boats from shore seems to be the most effective against a saturated attack, and has advantages over the barrier and random patrols due to the fact that the attacker will have to close in toward the defender in order to reach the asset being defended, bringing the attacker to the defender. A caveat is that this advantage may only be valid for defended assets that are confined in a small location

(less than 1 NM in the scenarios considered in this study), and there may not be an advantage if the assets stretch over a long coastline since the defender would not be able to guess exactly which point along the coast the attackers are heading for. Further exploration on tactics to defend a long coastline of assets could be worthwhile—for example, can a barrier patrol's effectiveness be increased if the patrol route were closer to shore than to the shipping lane in order to improve the intercept geometry?

3. Broader Operational Issues

This study has shown that having sufficient reaction time and being able to anticipate the attackers' direction of movement are key factors to a successful engagement. The security policies that are in place to control traffic and restrict approach routes are critical as a first filter to deduce the intent of the attacker. However, a major assumption was made concerning the actual engagement; that is an engagement can succeed so long as the patrol boat is sufficiently near to the attacker. Throughout the discussion, several crucial factors hindering a successful engagement were highlighted, such as the inaccurate firing of weapons due to the instability of the moving boats and the high-speed nature of the engagement leading to a tail-chase situation, which means that there is no guarantee of successful engagement when a patrol boat gets close to the attacker. Hence, the results presented in this study are optimistic, and boat-to-boat engagements taking place in reality would be expected to perform much worse.

There are further pressing operational questions that arise from these observations regarding actual existing engagement capabilities and CONOPS: how would a fully laden speedboat at full speed be stopped by a similar-sized patrol boat? A small, agile patrol boat may be able to give chase and catch up with the attacker, but could easily overturn in a collision or carry insufficient weaponry to stop the attacker. Conversely, a heavy patrol boat would be more survivable in the event of a collision and can carry more weapons, but would it be agile enough to maneuver and close in on the attacker? These questions beg additional research for insight.

B. COMPARISON OF TOOLS

Abdul-Ghaffar's prior research, which catalyzed this study, showed the application of modeling as a prescriptive tool, prescribing the deployment of patrol boats to ensure optimal detection of the threat. This study expands on prior research and illustrates the use of modeling and simulation as a facilitative tool for analysis, gaining insight by comparing various tactics and showing the utility of analyzing the robustness of a solution in the interception of the threat.

The solutions prescribed by Abdul-Ghaffar's analysis that promised 100% detection were not necessarily optimal when the MOE was changed to interdiction. There are alternative deployment tactics that were found to be essentially as good at detecting the threat, but better at interception of the threat. This finding agrees with Abdul-Ghaffar's conclusion of the further need to solve for patrol locations after his first step of analyzing the detection capability of patrol boats, and reinforces the importance of considering the effectiveness of both detection and interception for best tactic selection in patrol boat operations against the small boat attack threat.

The procedure to develop a realistic simulation involves a comprehensive survey of the factors and interactions in a scenario. This process, combined with the interpretation of the simulation results and, especially, with experienced personnel, can spotlight key uncertainties or assumptions about real world operating scenarios. In this study, the true capability of the patrol boats in engaging moving boats and the uncertainty of knowing the attacker's true target (if the defended assets are spread over a large area) were two key issues that were brought into focus.

C. FURTHER RESEARCH

Further research on the following areas could yield additional interesting insights relevant to the defense against small boat attacks:

- Compare the effectiveness of a mix of deployment tactics,

- Study the effectiveness of defense when defended assets are spread out over a longer coastline,

- Analyze alternative platforms and weapons, in particular, it would be possible to data-farm the parameters held constant or not considered in this study to suggest possible platform-weapon systems for effective threat mitigation,

- Analyze the effect of shipping density on defending against small boat attacks,

- More closely study the means to determine threat intent, and their effects on the concepts of operations for defending assets,

- Include shore-based assets (e.g. sensors) into the analysis, and

- Study factors and tactics to defend moving (passenger) ships from small boat attacks.

LIST OF REFERENCES

Abdul-Ghaffar, A.M. (2008). *Optimal Employment of Port Radar and Picket Ships to Detect Attacker Speedboats—A Defender-Attacker Optimization Model to Enhance Maritime Domain Awareness.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Department of Homeland Security, United States (2008). *Small Vessel Security Strategy*. Retrieved from www.dhs.gov/xlibrary/assets/small-vessel-security-strategy.pdf

GAMS (2008). GAMS Development Corporation, Washington, DC.

Google Earth. Retrieved Oct 5, 2010 from http://earth.google.com.

Hong Kong Port Development Council. *Hong Kong Port Facilities*. Retrieved Oct 25, 2010, from www.pdc.gov.hk/eng/facilities/port.htm.

Lalis, Vasileios (2007). *Exploring Naval Tactics with UAVs in an Island Complex Using Agent-Based Simulation.* Master's thesis, Naval Postgraduate School, Monterey, CA.

List of Singapore police officers killed in the line of duty. Wikipedia. Retrieved Nov 2, 2010, from http://en.wikipedia.org/wiki/List_of_Singapore_police_officers_killed_in_the_line_of_duty.

McIntosh, G. C., Galligan, D. P., Anderson, M. A., & Lauren, M. K. (2007). MANA user's manual. Defense Technology Agency, Auckland, New Zealand.

Naval Operations Analysis (3rd Ed). (1999). Annapolis, Maryland: Naval Institute Press. Naval Operations Analysis (3rd Ed). (1999). Annapolis, Maryland: Naval Institute Press.

Naval Operations Analysis (3rd Ed). (1999). Annapolis, Maryland: Naval Institute Press.

Port of Los Angeles. *Controlled Navigation Areas*. Retrieved Oct 25, 2010, from http://www.portoflosangeles.org/security/cna.asp.

Skolnik, M. I. (3rd Ed). (2002). Introduction to Radar Systems. New York: McGraw-Hill.

Tiburcio, F.M. (2005). *Maritime Protection of Critical Infrastructure Assets in the Campeche Sound*. Master's thesis, Naval Postgraduate School, Monterey, CA.

United States Coast Guard. *Boats*. Retrieved Sep 30, 2010, from http://www.uscg.mil/datasheet/25rbs.asp.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr Thomas Lucas
   Naval Postgraduate School
   Monterey, California

4. Professor Gerald Brown
   Naval Postgraduate School
   Monterey, California

5. Dr Robert Dell
   Naval Postgraduate School
   Monterey, California

6. Jeffrey Kline
   Naval Postgraduate School
   Monterey, California

7. Ed Lesnowicz
   Naval Postgraduate School
   Monterey, California

8. Wendy Walsh
   Naval Postgraduate School
   Monterey, California

9. Charles Hutching
   Department of Homeland Security

10. Professor Tat Soon Yeo
    Director, Temasek Defense Systems Institute (TDSI)
    National University of Singapore
    Singapore

11. Tan Lai Poh (Ms), Assistant Manager
    Temasek Defence Systems Institute
    National University of Singapore
    Singapore